A14 Ins

CLAIMS ~~CLAIMS~~

What is claimed is:

sub A16 1. In a computer system including at least one client computer coupled by a communications network to a secure storage facility located remotely to the client computer, a method of accessing a dedicated data storage unit, the data storage unit for storing data files associated with a user identification code in a secure environment, the method comprising the following steps:

initiating a request for accessing a dedicated data storage unit, the request specifying at least a remotely located secure storage facility containing the dedicated data storage unit and a user identification code, the secure storage facility associated with an address on a communications network;

in response to the request, automatically connecting to the remote secure storage facility at the associated address;

transmitting the request to the remotely located secure storage facility;

identifying the dedicated data storage unit associated with the specified user identification code; and

granting access to the identified dedicated data storage unit.

2. The method as in Claim 1 wherein the step of granting access includes granting access to the identified dedicated storage unit in accordance with pre-existing instructions associated with the specified user identification code.

3. The method as in Claim 1 wherein the request further specifies a processor identification code associated with a client computer, the step of identifying the dedicated data storage unit including identifying the dedicated data storage unit associated with both the specified user identification code and the specified processor identification code.

4. The method as in Claim 1 including the further step of displaying to a user a directory of data files stored in the dedicated data storage unit.

5. The method as in Claim 4 including the further steps of:

selecting a data file from the displayed directory of data files; and

transmitting the selected data file to a client computer associated with the request.

6. The method as in Claim 1 wherein each data file stored in the dedicated data storage unit has a predetermined security level assigned thereto, each data file being encrypted in accordance with its assigned security level.

7. The method as in Claim 1 wherein the request further specifies at least one data file stored on the identified dedicated data storage unit, the method further comprising the step of transmitting the specified at least one data file to a client computer associated with the request.

8. The method as in Claim 1 wherein each data file stored in the dedicated data storage unit is assigned a reference identification number by the secure storage facility at the time each data file is initially stored in the dedicated data storage unit.

9. The method as in Claim 8 wherein each data file stored in the dedicated data storage unit is assigned a new reference identification number by the secure storage facility each time the data file is accessed by a user after being initially stored in the dedicated data storage unit.

10. The method as in Claim 1 including the further steps of:

storing one or more data files in the dedicated data storage unit after access has been granted; and

encrypting the data in the one or more data files in accordance with a user assigned security level associated with each data file to be stored.

11. The method as in Claim 10 wherein the step of encrypting the data includes the step of encrypting the data at the secure storage facility prior to storing the one or more data files in the dedicated data storage unit.

12. The method as in Claim 11 wherein the step of encrypting the data includes the step of encrypting the data at a client computer associated with the request prior to storing the one or more data files in the dedicated data storage unit.

13. In a computer system including at least one client computer coupled by a communications network to a secure storage facility located remotely to the client computer, the remote secure storage facility identified by an address on the communications network and including at least one dedicated data storage unit for storing data files associated with a user identification code in a secure environment, encryption/decryption means and processor means, the remote secure storage facility adapted to allow access to the at least one dedicated data storage unit in accordance with a set of pre-existing instructions, apparatus for accessing the at least one data storage media such that the remote secure storage facility is transparent to a client computer, the apparatus comprising:

a logical data storage peripheral coupled to a client computer, the logical data storage peripheral associated with a remote secure storage facility; and

a controller associated with the logical data storage peripheral and storing the address on the communications network of at least one remote secure storage facility, the controller including machine executed means for:

receiving a request from a user on the client computer to access the logical data storage peripheral, the request specifying at least the logical data storage peripheral and a user identification code;

determining the address of the specified secure storage facility;

automatically connecting to the remote secure storage facility;

transmitting the access request to the remote secure storage facility; and

when access to a dedicated data storage unit associated with the specified user identification code has been granted, providing access to the dedicated data storage unit by routing communications between the client computer and the remote secure storage facility, the client computer unaware it is in communication with the remote secure storage facility.

14. Apparatus as in Claim 13 further comprising encryption and decryption means for encrypting data files to be stored in a dedicated data storage unit and decrypting data files retrieved from a dedicated data storage unit.

15. Apparatus as in Claim 14 wherein a data file to be stored in the dedicated data storage unit associated with a user identification code is encrypted in accordance with a user assigned security level.

16. Apparatus as in Claim 13 further comprising memory means for storing at least one directory, each directory containing a listing of data files stored in a dedicated data storage unit.

17. A secure storage facility having an address on a communications network and adapted for communication with other devices on the communications network, the secure storage facility comprising:

one or more dedicated data storage units for storing data files in a secure environment, each of the dedicated data storage units identified by at least one user identification code; and

a processor coupled to each of the dedicated data storage units, the processor including machine executed means for:

receiving an access request from a user on a remotely located client computer, the access request specifying at least a user identification code;

identifying a dedicated data storage unit associated with the specified user identification code; and

granting access to the identified dedicated data storage unit in accordance with a set of instructions associated with the specified user identification code.

18. A secure storage facility as in Claim 17 further comprising encryption and decryption means for encrypting and decrypting data files associated with a user identification code in accordance with the set of instructions associated with the user identification code.

19. A secure storage facility as in Claim 18 wherein a data file to be stored in the dedicated data storage unit associated with a user identification code is encrypted in accordance with a user assigned security level.

20. A secure storage facility as in Claim 17 wherein the set of instructions associated with a user identification code specifies read-only, write-only or read/write access to data files stored in the dedicated data storage unit associated with that user identification code.

Add A16